

# **PKI - The timid past and a promising future**

**- B. Robert Raja**

**ODYSSEY TECHNOLOGIES LIMITED**

1976 - 2022

# 1976-Birth of asymmetric crypto

- In 1976, the world had already entered the electronic age
- Supersonic jets and Inter-Continental missiles were there
- Other goodies out of war-time technology research
- Digital cryptography was just making its entrance – only symmetric
- Diffie and Hellman published their paper on ...



# New Directions in Cryptography

*Invited Paper*

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

**Abstract**—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

## I. INTRODUCTION

**W**E STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.


Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channels

# 1977

- Diffie's work was quickly followed by Rivest, Shamir and Adleman
- First practical asymmetric cipher
- Arguably the most important event in the history of Cryptography
- Charles Simonyi, computer scientist felt it was the most important event in 2000 years – not just in cryptography!

## Edge : 1999 Annual Question

### *What is the most important invention in the past two thousand years?*



"In the spirit of completeness and risking chronocentrism big time, I nominate Public Key Cryptosystems as something invented during the last two thousand years and which will remain useful long after the printing press will exist only in the (electronic) history books next to the steam engine. PKC has three incredible properties: perfect privacy, perfect authentication, and a reliable carrier of value and contracts — like gold used to be. All this in the digital environment where information can be easily and perfectly stored and copied. At a single stroke PKC transformed our vision of the asymptotic result of information technology from the 1984-ish nightmare to a realistic and ultimately attractive cyberspace where identity and privacy are not lost, despite of our (and Orwell's) commonsense intuition to the contrary"

- *Charles Simonyi*

*Former chief architect of Microsoft &  
Inventor of the Hungarian notation*

# 1978-1988

- The algorithm and its usage were strictly controlled by the US Federal Government
- Significantly inhibiting its usage in the world outside U.S Military
- No processes or formats were evolved for a decade
- Until CCITT defined X.509 ...



INTERNATIONAL TELECOMMUNICATION UNION

**CCITT**

THE INTERNATIONAL  
TELEGRAPH AND TELEPHONE  
CONSULTATIVE COMMITTEE

**X.509**

(11/1988)



# The next decade

- X.509 did not exactly set the world on fire!
- It was structured as an extended telephone directory entry – which in a sense it was
- Some interest in message protection on the ARPAnet/early internet was there
- eCommerce, eGovernance and authentication on the internet were not serious objectives

# Tyranny of x.509

- Protocols and processes for regulating its use made their slow appearance
- In most cases, the motive was to restrict the benefits to a few commercial and government interests
- Colourless applications and monotonous key interfaces
- Larger adoption of public keys remained a dream

# What should have been a veritable buffet...





...was turned into a poor man's soup kitchen

# The present state

- PKI is caught in a few narrow application spaces with the Government as the relying party
- Other domains find PKI difficult to adopt
- The one-size fits all certificates are inadequate
- Attribute certificates are proposed in the RFCs but not practical to implement

# Making PKI ubiquitous

- Time to remove the inhibitors
- All the benefits of Public keys need to be taken to the user community
- Role of PKI in a digital society has to be reappraised
- Calls for changes in approaches to technology and implementation
- Most importantly, a change in mindset

# Need 1 - Private Key

- Private Key should always be in owner's absolute possession and control
- Constructive Possession for digital objects is a preposterous notion
- Any signature scheme that does not put the key in the sole and exclusive physical possession of the signer will nullify the benefits of a public key system
- Succumbing to temporary exigencies or short term commercial interests will eventually kill PKI

# Need 2 – Attribute Certification

- The attribute certificate model in the RFC is impractical
- X.509 and the CA system to remain the root of trust with spontaneous trust nodes below them
- Insistence on certificates must go – attributes can be tied to signatures of entities – ensuring flexibility
- A hospital can amplify a doctor's signature with her specialization; a university can reinforce a researcher's signed paper by countersigning his qualifications
- Purely digital societies cannot be formed without attribute assurances across the network



## Need 3 – Simpler key usage

- Another major obstacle to large scale user adoption
- The device space has seen tremendous advances
- Devices abound – in people’s pockets and bodies
- PKI is sticking to archaic devices and OS and application interfaces
- This is a call for creating secure devices and interfaces that are easy to use – not to compromise security in the name of ease of use

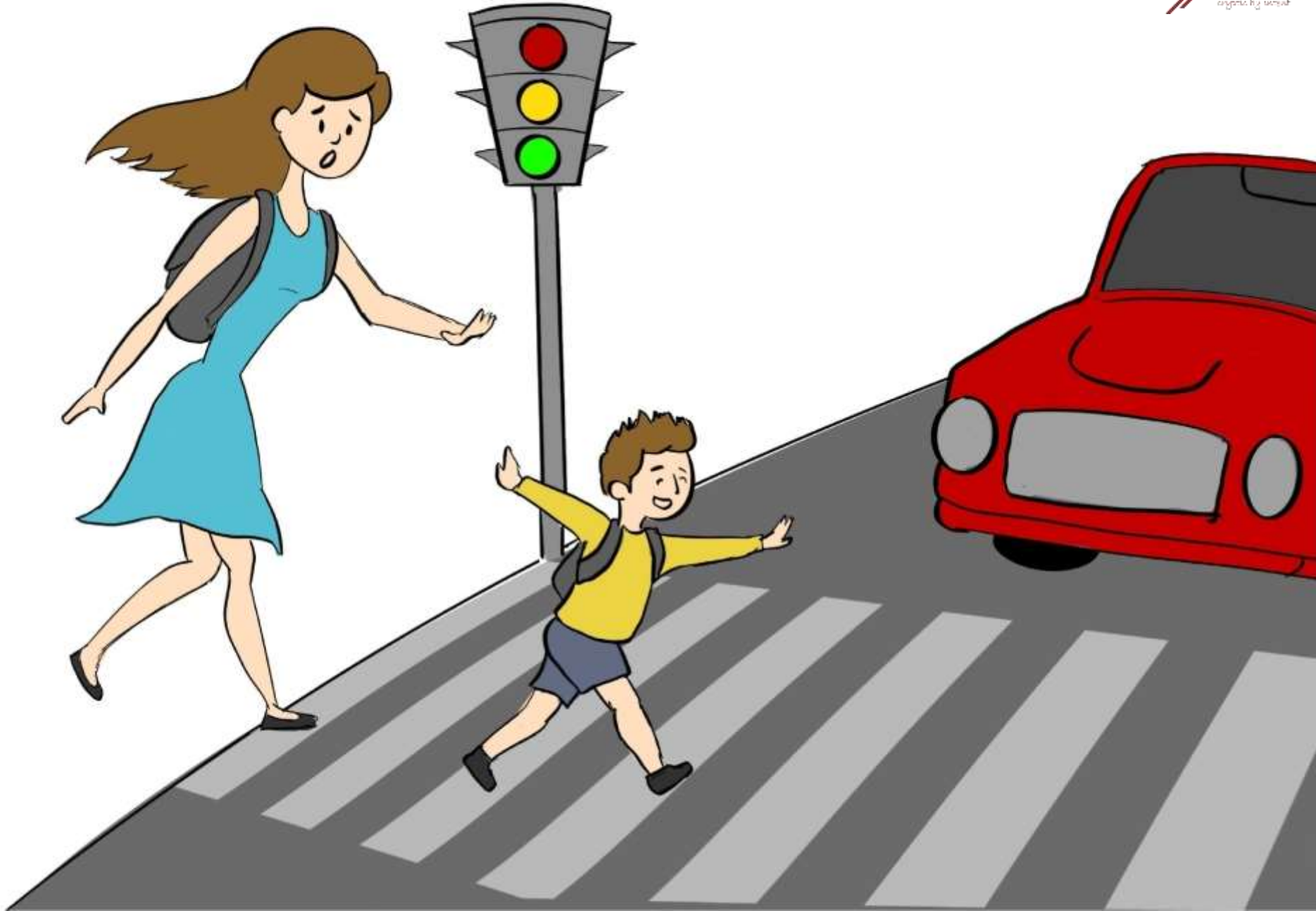
## Need 4 – A proper presentation

- Should be properly presented to the aspiring digital population
- Making a big virtue of non-repudiation should go
- It may be attractive to a few relying parties but it is insulting to the subscriber
- We do not generally hear of people repudiating their own actions maliciously – We repudiate when someone else has impersonated us!
- This is an example but the overall presentation of PKI to the populace should be rethought

# Need 5 – Compliance and Security

- It is important to prepare citizens for a fully digitized society
- Norms of behaviour and etiquette in digital space is the same as physical space – except in the technical details
- In society most people behave properly – not out of fear of law but because they know it is the norm
- Overemphasis on legal-compliance and legal-acceptance must go! – It intimidates and scares the users away!

Common sense can tell you what is secure



# The future

- We have outlined some of our thoughts collected over the years
- Public Keys are the only way to retain a digital society's fabric and ensure its survival
- There is a huge role for all of us if we choose the right path

# Thank You



**ODYSSEY TECHNOLOGIES LIMITED**

5th Floor, Dowlath Towers, 63, Taylors Road, Kilpauk,  
Chennai - 600010 , India.

[sales@odysseytec.com](mailto:sales@odysseytec.com)

[www.odysseytec.com](http://www.odysseytec.com)

+91 44 26450082/83